METHOD AND DEVICE FOR RENDERING THE PROTECTION OF ELECTRONIC DATA AGAINST PIRATE COPYING IN A NETWORK MORE EFFECTIVE AND AVOID FILTERING SYSTEMS

TECHNICAL FIELD

A method for rendering the protection of electronic data against piracy copying in networks more effective and for avoiding filtering systems by providing said data in a plurality of physical computers. Musical compositions, movies and other similar intellectual creations normally are stored in digital form on electronic or optical media. As the digital form of storing allows copying and distribution without quality deterioration there is an extensive distribution of such data over the Internet and through other channels. To some extent the distribution takes place under control of the proprietors of the rights associated to the intellectual creations but to a large extent without such control and without leading to any kind of compensation to the proprietors of the rights for the use following the distribution. The intellectual creations normally are copyright protected or protected by other means. The invention relates also to a device for using the method.

PRIOR ART

It has turned out to be very difficult to completely prevent an undesired distribution of protective works in spite of the use of copying protection and other forms of electronic protection. By using the Internet and different types of network systems, such as for instance peer-to-peer and other decentralized networks it has also turned out to be possible to avoid some legal protection for copyright protected works that are distributed as computer files.

A network of peer-to-peer type is a decentralized network and is designed in such a way that a plurality of computers are connected through a net, for instance Internet, in such a way that the information stored in files in the computers are shared and kept publicly available for any users of the network. A legally copied file intended for personal use and comprising a song or a video movie can be reached from and transferred to any arbitrary computer in a network by uploading the file.

In an attempt to limit the distribution of copyright protected works there has been suggested a method based on the fact that incomplete computer files or computer files with corrupted information content are distributed on purpose by the proprietors of the rights or by another party. As a result of providing a plurality of versions of a work after the distribution it is assumed that the interest of acquiring the work in an unauthorized way will be lower because there is a considerable chance that a computer file downloaded unauthorized will be corrupted.

One example of deteriorating the information content is disclosed in US2002/0082999. In this document it is shown generally also how files with deteriorated content are stored in a plurality of computers. The computers are connected to a network of peer-to-peer type and therefore are capable of distributing the files to other computers of the network. To achieve the best effect, that is to ensure that a large part of the files that are available on the network are deteriorated, it is suggested in US2002/0082999 that the distribution of the deteriorated files starts before any computer files with correct content are available. Even if the distribution starts before the start of sale of correct computer files such as CD-records and DVD-movies, it happens that the correct file is distributed even earlier. To reduce the effect of such a distribution it is suggested in US2002/0082999 to initially start corrupting versions of a correct file already distributed from an unauthorized source in the same way and that these versions are distributed thereafter.

The computers used for providing and as a result also distributing files with corrupted content should be provided in large numbers to make the distribution effective. However, a large amount of computers will increase the costs. By analyzing in different ways the computers distributing files over for instance Internet it has been discovered that it is possible to locate computers used for distributing corrupted files. One possible way of analyzing is to examine the files that are stored and available in the computer. The identity of these computers can be defined by the IP number used by the computer during communication through the Internet. If the IP number is revealed for instance by a continuous analyze of the content of the shared folders and the function of the computer during distribution is revealed, it can be filtered of other computers and has a result be prevented from taking part of the distribution of corrupted files, which is advantage in the efforts of obstructing unauthorized distribution of computer files.

SUMMARY OF THE PRESENT INVENTION

An object of the invention is to avoid the above mentioned disadvantage and to provide a method and a device rendering possible an efficient distribution of files with a corrupted content with a limited chance of discovery. This object is achieved by providing to the computers arranged to distribute files IP numbers selected from a number of IP addresses which number is substantially larger than the number of distributing computers. The selection takes place without a specific order or randomly so as to avoid groups of IP addresses or IP addresses in consecutive order. The computers distributing the damaged files will in this context operate as disturbance computers.

A plurality of computers are used simultaneously and a plurality of network clients, that is software sharing folders and by other means providing the corrupted computer files, can be executed in each disturbance computer. By using a plurality of network clients in each disturbance computer the distribution can be increased without the need to use a plurality of physical computers. The pace of distribution can be further increased by emulating in each of the physical computers a plurality of virtual computers. In such an embodiment each of the virtual computers, or groups of virtual computers, is provided with an IP address as described above. As a result a plurality of computers can operate with a common IP address towards the network.

An alternative or complement to emulated computers is to use software to intercept the communication of identical network clients with the operating system or function libraries of the computers, so as to avoid that different instances of the programs prevent each others function and as a result a plurality of network clients executing simultaneously in each computer is allowed.

Preferably the IP addresses of disturbance computers are tunneled so as to further obstruct the tracking of the computers. A frequent and an irregularly exchange of IP addresses also will improve the possibilities of maintaining the disturbance computers secret and prevent them from being tracked down and blocked. It can also be appropriate to use fire walls or other network protections between the disturbance computers and Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be further explained from the following detailed description taking in conjunction with the accompanying drawings, in which

Fig. 1 schematically shows a network of a plurality of interconnected computers in which network clients are executed for distributing computer files and,

Fig. 2 schematically shows the configuration of computers in a network.

DETAILED DESCRIPTION

In a practical embodiment in accordance with Fig. 1 a plurality of user computers 10 are connected to Internet 11. Some of the user computers will operate as so called super-peers, see description below with reference to Fig. 2. In the user computers a client software is executed to allow sharing, uploading and downloading of computer files, for instance including music.

The computers that are connected to Internet are all, as seen from the outside, provided with a unique IP address, which normally is provided by the Internet provider used by the user. At least in connection with transferring a computer file between two user computers these computers are connected to each other, as indicated in Fig. 1, to such an extent that a file transfer between the computers is possible.

A plurality of disturbance computers 12 are also connected to Internet. The disturbance computers can be arranged as individual physical computers or as virtual computers. A plurality of disturbance computers is gathered in a so called server park 19, which is connected to Internet through a fire wall 14. The disturbance computers 12 are also connected to Internet and are given IP addresses. When the IP addresses are assigned connected sequences and by other means interrelated IP addresses are avoided. Preferably IP addresses are selected randomly from a large set of addresses from an Internet provider intended for normal subscribers. The IP addresses preferably also are exchanged by irregular intervals so as to avoid

tracking and identification of the disturbance computers. The selected IP addresses are tunneled into the server park.

In the embodiment shown in Fig. 1 a plurality of client software 13 is executed in the disturbance computers 12, which can be servers. The client software 13 communicates with a corresponding client software in other computers 10 through Internet and thereby is capable of providing files with corrupted content. Each client software operates as a disturbance peer in this context.

Normally client software will use a full power of a modern server only during some percents of time when the program is active. In between the use of resources is down to a few percents. Unfortunately there are only a few types of client software of the type that can be executed simultaneously in the same computer. So as to utilize a physical computer to a maximum extent and reach the best possible cost efficiency a plurality of virtual or emulated computers should be executed in each physical computer. In a start up scenario 35 servers with 50 virtual computers in each server the result will be 1750 disturbance computers to a fraction of the costs that otherwise should have been necessary for purchasing, management etc.

One of the disturbance computers consists of a physical computer and emulating software executing in the computer. The emulating software makes the physical single computer acting as a plurality of virtual computers 15. Each of the virtual computers then can execute a plurality of client software and as a result further increase the number of operating disturbance peers.

Existing protocols for tracking computers, such as ICMP TRACEROUTE, are prevented from detecting the disturbance computer by the use of a fire wall and/or disturbance software.

A first arbitrary computer 16 executing client software for communicating between computers connected in a network of peer-to-peer type can be connected to a disturbance computer including a first disturbance peer 17. Is should be noted that networks of peer-to-peer type in this context include also functionally similar file sharing networks. By the IP number selected for the disturbance peer the computer 16 appears to be connected to another fictitious computer 18, but is instead connected to a computer in the server park 19 through the fire wall 14. In a similar way a second arbitrary computer 20 is connected to a second disturbance peer 21,

but also seems to be connected to a fictitious computer 22, and a third arbitrary computer 23 with a third disturbance peer 24 even if this computer can be considered connected to a further fictitious computer 25.

In connection with transferring a corrupted file from a disturbance peer the transfer is recorded. Data related to transfers is stored in a data base 26 in the server park. The disturbance peers are controlled by a central unit 27 in the server park. The central unit 27 reads data stored in the data base and calculates the distributing effect and other relevant results of the work of the disturbance peers. Calculated and received information are preferably also stored as time goes on in a data base.

Fig. 2 shows schematically the shape of a decentralized network. A plurality of computers 10 is included in the network and the computers are organized in peer groups 29 around so called super-peers 28. A computer 10 reaches other computers for transferring computer files as described above only through the super-peer 28 that the computer is connected to. Normally a computer is connected only to one super-peer. The first super-peer 17 is connected to a super-peer 28 in the same manner as other computers connected to the super-peer and behaves in the same way as such a computer to other computers as well as to the super-peer. Correspondingly the second disturbance peer 21 and the third disturbance peer 24 are connected to the super-peer 28. It may be that a plurality of disturbance peers 24 is associated or connected to the same super-peer since the configuration takes place without knowledge of and without regard to whether computers are disturbance peers.

Disturbance peers are controlled by the central unit 27 and the information stored in a data base 26. Programmed blocks of activities can be activated either for single peers, groups of peers or for all peers. Such activities include the change of super-peer, or restarting the virtual computer. The software used in the disturbance peers and the virtual computers preferably is identical so as to be updated in a simple manner by means of conventional or specifically adapted network tools.

A method for measuring the efficiency of disturbances can be to search among random or selected super-peers for the protected works. Then data in the search results are compared and an efficiency percentage can be calculated. During this process it is possible also to note the extent of the secondary disturbance effect, the

so called piggybacking, that is the effect that is a result of a plurality of persons downloading files with corrupted content when looking for "original" files do not remove the files and then themselves continue to function as external disturbance peers. The secondary disturbance effect can be added to the previously determined value and a result, such as the total number of downloaded files with corrupted content, can be calculated and statistically presented.